UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/591,786	09/05/2006	Sebastien Canard	33901-220PUS	4281

7590 04/11/2012

Thomas Langer
Cohen Pontani Lieberman & Pavane
Suite 1210
551 fifth Avenue
New York, NY 10176

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/11/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/591,786	CANARD ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2012*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-4,9-18,20 and 22-29* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) *29* is/are allowed.

7)☒ Claim(s) *1-4,9-18,20 and 22-28* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to amendment filed on 1/24/2012. Claims 5-8, 19 and 21 have been canceled. Claims 1, 10-18, 23 and 25-28 have been amended. Claim 29 is new. Claims 1-4, 9-18, 20 and 22-29 are now pending,

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 12, 14, 16 and 18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The Examiner notes that the claims are directed to a "computer program" as the Examiner notes that the MPEP requires that a "computer program" be resident to a "computer readable medium" to be considered statutory subject matter. Additionally the Examiner notes that the applicant must explicit recite that the "medium" is non- transitory signals.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 10 -14 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fujioka et al. (US Patent No. 6,845, 447 and Fujioka hereinafter) in view of Jorba et al. (US Patent Publication No. 2005/0021479 and Jorba hereinafter) and further in view of Jakobsson et al. (US Patent No.6,636,939 and Jakobsson hereinafter).

1. As to claims 1, 10 -14 and 28, Fujioka teaches a electronic voting method, comprising the steps of: obtaining from a signer apparatus, according to a fair blind signature scheme (i.e.,. ..teaches the use of a blind signature scheme [abstract., lines 1-7],

a digital signature (yi) of a data signal (xi) generated from a voter apparatus (i.e., …teaches generating a digital signature [col. 5, lines 25-30] and a encrypted vote (e.g., data signal) [col. 5, lines 15-25]), said data signal comprising an encrypted vote (vi) of a voter (i.e.,...teaches a encrypted vote [col. 5, lines 15-25]; and establishing, at a trusted authority apparatus, a link between a data pair (xi, yi) comprising said data signal and said digital signature (i.e., …teaches (zi, yi) where zi is the encrypted vote and yi is the signature [col. 5, lines 46-50]),

and a signing session in which said data pair (xi, yi) was generated (i.e., …teaches generating a (zi, yi) where zi is the encrypted vote and yi is the signature [col. 5, lines 46-50]),

The Examiner notes with regards to applicant's claim limitation of a fair blind signature scheme permitting establishment of the link via a signature tracing mechanism included in the fair blind signature scheme, the applicant is noted to disclose in paragraph 18 the following: :"… fair blind signature schemes enable a given digital signature to be linked to a given user". While Fujioka is noted to teach a blind signature scheme, Fujioka's teachings do not expressly disclose applicant's claim limitation element of permitting establishment of the link via a tracing protocol included in the fair blind signature scheme. In this instance the Examiner notes the teachings of Jorba. Jorba is noted to teach a blind signature scheme comprising a verification protocol (e.g., tracing protocol) where a link ballot identifier is used for tracability purposes. See Jorba paragraph 123. Therefore given the system described above by Fujioka, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance process integrity by employing Jorba's verification protocol as described above.

The Examiner notes that while the combination of Fugoka and Jorba discloses applicant's claim limitation element of a fair blind signature scheme permitting establishment of the link via a signature tracing mechanism included in the fair blind signature scheme the Examiner notes that neither reference disclose applicant's newly amended claim limitation of:said signature-tracing mechanism enabling the trusted authority to identify, based on a transcript of said signing session, the data pair(x_i, y_i) generated during said signing session. However n this instance the Examiner notes the

teachings of prior art reference Jakobsson. Jakobsson is noted to teach a transcript tracing based method, where transcripts are used to identify a proper signature. See Jakobsson col. 4, lines 1-10. The Examiner note that Therefore given the system described above by Fujioka and Jorba, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance signature integrity by employing Jakobsson's use of transcript related data to verify signature data as described above.

2. As to claim 2, the system of Fujioka disclose the use of a fair blind signature scheme, however the system does not expressly teach voting method where the fair blind signature scheme comprises a threshold fair blind signature scheme in which the digital signature is generated by cooperation of a number t of n servers, where t n, and where n - t + 1 servers need to be honest. However in this instance the Examiner notes the teachings of Jorba. Jorba is noted to discloses in paragraph 7 the following: " A cryptographic voting scheme accurately determines the steps and actions involved in the remote vote casting as well by the device issuing the votes used by the voter as by the corresponding voting server. The scheme also determines the cryptographic operations which must occur during the process of vote tallying and also for verifying the final results. Of course, a cryptographic voting scheme must also be completed with generic safety measures to maximise the safety and to best protect the full voting system. Therefore given the system described above by Fujioka, a person of ordinary skill in the art would have recognized the advantage of modifying a system to

enhance process integrity by employing Jorba's verification protocol as described above.

5-8 (Cancelled).

3. Claims 3, 15-18 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fujioka in view of Jorba as applied to claim 1 above, and further in view of Juang et al. (NPL " A Verifiable Multi-Authority Secret Election Allowing Abstention from Voting.(Juang hereinafter) (cited from IDS (date 9/15/2006)).

4. As to claims 3 and 22, Fujioka teaches a voting method where the data signal (x/) corresponds to the encrypted vote (vi) of the voter which is encrypted according to a first encryption scheme (ErM) (i.e., …teaches encrypted vote [col. 5, lines 15-25]),

With regards to applicant's claim limitation of:

said first encryption scheme being the encryption scheme of a first mix-net (TM) contained in a vote-tallying module, the Examiner notes that neither Fujioka nor Jorba discloses the elements as recited in the above claim limitation. However in this instance the Examiner notes the teachings of prior art Juang specifically paragraph 3.3. Juang is noted to teach the use of mix-net in a voting process. Therefore given the system described above by Fujioka and Jorba, a person of ordinary skill in the art would have

recognized the advantage of modifying a system to enhance data security by employing Juang 's mix-net process as described above.

5. Claims15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fujioka and Jorba in view of Jakobsson, and further in view of Juang.

6. As to clams 15 and 16, Fujioka teaches a voting system ballot-order-randomizer module comprising a processor configured to provide:

input means for receiving a batch of cast votes, each cast vote comprising an encrypted data signal (ci) comprising data (xi) indicative of a respective vote (vi) of a voter which is digitally signed according to a fair blind signature scheme (i.e.,. ..teaches the use of a blind signature scheme [abstract., lines 1-7] …further teaches generating a digital signature [col. 5, lines 25-30] and a encrypted vote (e.g., data signal) [col. 5, lines 15-25])),

each encrypted data signal (ci) being encrypted according to a predetermined encryption scheme (EM) [col. 5, lines 15-25]);

With regards to applicant's claim limitation of, “said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated”, the applicant is noted to disclose in paragraph 18 the following: :”… fair blind signature schemes enable a given digital signature to be linked

to a given user". While Fujioka is noted to teach a blind signature scheme, Fujioka teachings do not expressly disclose permitting establishment of the link via a tracing protocol included in the fair blind signature scheme. In this instance the Examiner notes the teachings of Jorba. Jorba is noted to teach a blind signature voting scheme comprising a verification protocol (e.g., tracing protocol) where a link ballot identifier is used for tracability purposes. See Jorba paragraph 123. Therefore given the system described above by Fujioka, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance process integrity by employing Jorba's verification protocol as described above.

and output means for outputting the decrypted signals of said batch of cast votes in an order different from the order of corresponding encrypted data signals in said batch of cast votes (i.e…. the Examiner notes fig 5 of Fujioka where Fujioka illustrates a decryptor and outputting the decrypted encrypted vote signals).

The Examiner notes that while the combination of Fugoka and Jorba discloses applicant's claim limitation element of a fair blind signature scheme permitting establishment of the link via a signature tracing mechanism included in the fair blind signature scheme the Examiner notes that neither reference disclose applicant's newly amended claim limitation of: said signature-tracing mechanism enabling the trusted authority to identify, based on a transcript of said signing session, the data pair(x_i, y_i) generated during said signing session. However n this instance the Examiner notes the teachings of prior art reference Jakobsson. Jakobsson is noted to teach a transcript

tracing based method, where transcripts are used to identify a proper signature. See Jakobsson col. 4, lines 1-10. The Examiner note that Therefore given the system described above by Fujioka and Jorba, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance signature integrity by employing Jakobsson's use of transcript related data to verify signature data as described above.

The combined teachings of Fujioka, Jorba and Jakobsson are noted to teach decrypting a encrypted data signal (e.g. vote) by applying a decryption scheme. See figure 5 of Fujioka. However the combined teachings of both references do not expressly teach applicant's usage of a mix-net as recited in applicant's claim limitation element "a mix-net (M) for decrypting said encrypted data signals (ci) by applying a decryption scheme (DM) which is an inverse of said predetermined encryption scheme (EM); However in this instance the Examiner notes the teachings of prior art Juang specifically paragraph 3.3. Juang is noted to teach the use of mix-net in a voting process. Therefore given the system described above by Fujioka, Jorba and Jakobsson, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance data security by employing Juang 's mix-net process as described above.

7. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fujioka in view of Jakobsson, and further in view of Juang.

8. As to clams 17 and 18, Fujioka teaches a voting system ballot-order-randomizer module comprising a processor configured to provide:

input means for receiving a batch of cast votes, each cast vote comprising an encrypted data signal (ci) comprising data (xi) indicative of a respective vote (vi) of a voter which is digitally signed according to a fair blind signature scheme (i.e.,. ..teaches the use of a blind signature scheme [abstract., lines 1-7] …further teaches generating a digital signature [col. 5, lines 25-30] and a encrypted vote (e.g., data signal) [col. 5, lines 15-25])),

each encrypted data signal (ci) being encrypted according to a predetermined encryption scheme (EM) [col. 5, lines 15-25]);

With regards to applicant's newly amended claim limitation of, “said fair blind signature scheme having a signature tracing mechanism which enables a trusted authority apparatus to identify based on a signing session data pair (x_i, y_i) generated”, the Examiner notes in this instance the teachings of prior art reference Jakobsson. Jakobsson is noted to teach a transcript tracing based method, where transcripts are used to identify a proper signature. See Jakobsson col. 4, lines 1-10. The Examiner note that Therefore given the system described above by Fujioka, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance signature integrity by employing Jakobsson’s use of transcript related data to verify signature data as described above.

The combined teachings of Fujioka and Jakobsson are noted to teach decrypting a encrypted data signal (e.g. vote) by applying a decryption scheme. See figure 5 of Fujioka. However the combined teachings of both references do not expressly teach applicant's usage of a mix-net as recited in applicant's claim limitation element "a mix-net (M) for decrypting said encrypted data signals (ci) by applying a decryption scheme (DM) which is an inverse of said predetermined encryption scheme (EM); However in this instance the Examiner notes the teachings of prior art Juang specifically paragraph 3.3. Juang is noted to teach the use of mix-net in a voting process. Therefore given the system described above by Fujioka and Jakobsson, a person of ordinary skill in the art would have recognized the advantage of modifying a system to enhance data security by employing Juang 's mix-net process as described above.

19 (Cancelled).

21 (Cancelled).

Allowable Subject Matter

Claims 4, 9, 20 and 23-27, and 29 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

Examiner Remarks – Specification Objection

The Examiner withdraws the objection made to the specification in view of newly amended title.

Examiner Remarks - 35 U.S.C. §101,

The Examiner maintains the rejection under 101, citing that the MPEP requires claims drawn to a computer program explicitly recite that the computer program is resident to a “computer readable medium”. Additionally the Examiner notes the current office request applicants explicitly state as part of the claim language that the 'computer readable medium" is non-transitory.

Examiner Remarks - 35 U.S.C. §103(a),

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Flynn Nathan can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431